Domesticating data

Domesticating Data: Socio-Legal Perspectives on Smart Homes and Good Data Design

Martin Flintham, Murray Goulden, Dominic Price, Lachlan Urquhart

Introduction

In 2012, a New York Times story on the most banal of subjects - store card data - went viral. An American man, it was claimed, had discovered that his daughter was pregnant after a retail store began targeting the family with pregnancy-related products. The retail store had inferred the pregnancy through purchase patterns in the family's store card data. The algorithms knew before the girl's family did.

This story has commonly been read as a lesson in the power of Big Data to reveal our most intimate secrets. We see it as something different: a warning of a future in which the Internet of Things (IoT) creates torrents of *group data* that overwhelm the efforts of group members to manage the personal information that other members have access to. We call this group data *interpersonal data*[1], because it is drawn from, and carries consequences for, the relationships between intimate groups like the family above. Public discussions around the ethics of data have, to date, overwhelmingly focused upon what institutions - state or corporate - know about individuals. We do not deny the importance of this framing, but wish to complement it with a focus on what happens when data capture is no longer restricted to individuals' devices, but instead embedded in our social environments and involves multiple actors. What does 'good data' look like in this space defined by interpersonal relations, how good is it really, and how do we avoid it becoming 'bad data' through inappropriate design, or legal consequence?

In addressing this question, we focus on the 'smart home', as the archetypal group space into which the IoT is extending. After introducing the technologies which are currently being designed for this space, we turn our attention to how law regulates data in this space (or not). This focus reflects the importance of law in shaping the future design of technologies, through concepts like privacy by design. But just as importantly, it provides an example of the challenges that external frameworks have when engaging with domestic spaces. Our analysis is limited to European Union law, on the basis that, as the most proactive regulator in this space, the EU is highlighting the challenges that lie ahead for technology designers, and society more broadly.

We argue the 'goodness' of data in the home is strictly contextual. The socially complex nature of the domestic space means that, even with best intentions, good applications can result in bad outcomes if they do not attend to what users actually want and do in practice. For example, the Samaritans

[1] Goulden, Murray, Peter Tolmie, Richard Mortier, Tom Lodge, Anna-Kaisa Pietilainen, and Renata Teixeira. 2018. "Living with Interpersonal Data: Observability and Accountability in the Age of Pervasive ICT." *New Media & Society* 20 (4): 1580–99.

Radar[2] app garnered significant criticism by collecting, sharing and drawing attention to Tweets labelled as indicative of distress despite aiming to do good by preventing suicide. When designing for the home, there is clearly a need to engage with the setting, and actors therein. From the legal perspective, whilst GDPR may provide high level requirements and norms, these need to be appropriately and carefully situated so as not to become problematic themselves. As Nissenbaum has long argued, privacy can be seen as the contextual integrity of information, where harms occur if that information moves outside what individuals expect, to unanticipated channels of sharing.[3] Accordingly, within the home, to understand if applications will result in good or bad data they need to be designed with an appreciation of the expectations and uses *specific to* the practice(s) implicated by the data.

Viewed through the prism of interpersonal data, the specific forms of sociality in this space take on greater importance for design. Single-occupier homes are becoming more common, yet are still in the minority. Most homes are shared spaces, indeed even single-occupier homes may regularly host guests that otherwise live elsewhere. Most commonly, this sharing is between family members, though this itself is a concept which defies easy categorisation for technical systems. The once widespread notion of the family as a nuclear unit, clearly structured according to its social functions, and distinct from wider kin and community,[4] has little support today amongst those that study it. Instead, drawing on empirical study, family is seen as diverse, fluid and dynamic.[5,6] Defining what family *is* has accordingly become far less deterministic, based not on any applied template, but rather on *doings*[7] - in other words, the shared practices of members who identify as family. The notion of family and the experience of it are then co-producing. Families may fit the nuclear template, but they may also be made up of cohabiting couples, those 'living apart but together', they may be gay or lesbian. Agency in families is unevenly distributed, often along lines of generation and gender, but the specifics of the distribution are situated in the particular instance in question. In some cases, this distribution is so uneven it becomes coercive, and members subject to violence at the hands of other family members.[8] In their totality, these characteristics are deeply challenging for technological systems that rely on the application of machine-readable formal structures for their operations.

To explore what the outcomes of these technical and legal developments might mean for the home, we engage in *design fiction*. Design is commonly concerned with solving problems. Design fiction uses the same design practices but for asking questions instead. Through several short narratives, our design fiction seeks to show how the smart home might provoke unconsidered, problematic or unexpected data practices within the smart home. We draw on these to conclude with reflections on the specific but complex challenges that designers and participants of this new world face in trying to design good data practice, or at least in avoiding the bad.

---

[2] Jamie Orme, 'Samaritans pulls 'suicide watch' Radar app over privacy concerns', The Guardian, 7 November 2014, https://www.theguardian.com/society/2014/nov/07/samaritans-radar-app-suicide-watch-privacy-twitter-users.

[3] Helen Nissenbaum, 'Privacy As Contextual Integrity', *Washington Law Review* (2004): 79.

[4] Talcot Parsons, 'The American Family', in Talcot Parsons and Robert Freed Bales, *Family, socialization and interaction process.* Free Press, 1955.

[5] Deborah Chambers, *'A Sociology of Family Life'*, Polity Press 2012.

[6] David Cheal, *'Sociology of Family Life'*, Springer 2002.

[7] David Morgan, *'Family Connections: An Introduction to Family Studies'*, Polity Press 1996.

[8] Julia Wardhaugh, 'The Unaccommodated Woman: Home, Homelessness and Identity', *The Sociological Review* (2001) 47. 91 - 109. 10.1111/1467-954X.00164.

The Smart Home

The smart home marks a coordinated industry programme to bring IoT technologies, and the associated service platforms to which they connect, into the home. Smart devices span heating, security, entertainment, lighting and appliances, but the vanguard has proved to be the smart speaker. In 2017 it was predicted that smart speakers will be installed in over 60 million homes by the end of 2018[9], by summer 2018 it was predicted they would be in 100m homes[10]. Currently these devices' adoption is geographically limited to the most lucrative and accessible markets - Amazon's Alexa for example was, as of 2017, only available in English, German and Japanese (Google's offering covered an additional four languages). Their availability can be expected to expand greatly in the next five years however - whilst Apple lags in smart home offerings, it's voice assistant already covers 21 languages. In regards to data, the application of pervasive computing to such shared environments presents a qualitatively different set of challenges from designing discrete computing technologies for individual users, as the industry has done in the four decades since the computer was reconfigured as *personal*. In the existing era of personal devices, the challenge has been one of protecting personal data from 'bad actors' - third parties who would exploit that data for their own gain. The standard defence has been to secure such data behind a user account, gated by biometric data or a password, leaving the data only accessible to the user and the service provider.

In recent years this challenge has become increasingly fraught. First, a procession of large-scale hacks weakened the notion that user data was secure from third parties. The consequences of these hacks ranged from the inconvenience of required password changes, to credit card fraud, to - at least in the case of the Ashley Madison hack[11] - at least two suicides. More recently, the focus has turned away from third party interventions, to the intentions of the service providers themselves. At the time of writing the likes of Facebook and Google are facing intense pressure from the public, media and regulators over their own gathering and use of personal data.

In the coming era of the IoT the challenges posed by personal data collection remain, but are joined by those of interpersonal data. Data collected from, and actuated by, pervasive computing in the environments around us implicates not only the individual user of a device, but the multiple users of the space. In smart homes, as our focus is here, these multiple users have existing relationships, as families; flatmates; host-guests; owner-pets. Here the elegance of the secured user account solution breaks down. This approach is predicated upon the uncontroversial identification of data subject, which is to say the data collected from a device logged into a specific user account is assumed to belong to that user, and hence accessible to them alone.

---

[9] Associated Press, 'Smart Speaker Sales More Than Triple in 2017', Billboard, 28 December 2017, https://www.billboard.com/articles/business/8085524/smart-speaker-sales-tripled-25-million-year-2017.

[10] Bret Kinsella, 'Smart Speakers to Reach 100 Million Installed Base Worldwide in 2018, Google to Catch Amazon by 2022', Voicebot AI Blog, 10 July 2018, https://voicebot.ai/2018/07/10/smart-speakers-to-reach-100-million-installed-base-worldwide-in-2018-google-to-catch-amazon-by-2022/

[11] The Ashley Madison hack in 2015 saw the leaking of millions of users' details from the infidelity website (tagline: "Life is short. Have an affair"). In the aftermath, as well as suicides, there are reports of much larger numbers of users experiencing distress as they feared their loved ones would find out. Tom Lammont, 'Life after the Ashley Madison affair', The Observer, 28 February 2016, https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked.

In practice, within intimate settings this is already more complex than is acknowledged. The introduction of 'incognito' or 'private' browsing windows[12] is in part a reflection of the recognition that in settings like homes, devices are often shared, and that some users may wish to hide parts of their browsing history from subsequent users. Such a solution is problematic in that it requires the user remember to select the option every time they wish to avoid the risk of 'social surveillance'.[13] In the context of IoT it becomes even more problematic, because data collection is no longer so obviously tied to specific practices (e.g. browsing on a shared laptop), but is embedded in the world around us, potentially tracking us through every waking, and sleeping, moment. Temporarily 'opting-out' of tracking becomes unviable.

The specific danger here is not some distant bad actor accessing personal data, but rather its exposure to those closest to us. Our intimates may know more of our secrets than anyone else, but what we hide from them is that which is most potentially consequential. When people are asked about breaches of their privacy, it is not abstract third parties that concern them the most, but those they know best.[14,15] This appears born out by the suicides which followed the Ashley Madison hack, which revealed infidelity, or attempted infidelity, to users' loved ones. It is the potential breach of the trust held between these closest ties, and the consequences of such breaches, that makes such data exposure so troublesome.

The IoT raises questions of how such interpersonal data should be secured, but also how it should be used, for the use of data often entails exposure of it in some form. The content recommendation systems of video-on-demand services like Amazon Video, for example, reveal in their suggestions the type of content previously consumed. If, for example, a user had a preference for erotic content, this will be apparent on subsequent visits to the site by other members of the household.

Amazon is also the creator of Echo, which, along with Google's Home, has become front runner in the smart home market. Echo and Home have established their respective parent companies as the default platform providers in the smart home. Increasingly, other companies are integrating their devices into one or both platforms. As such, Amazon and Google find themselves at the sharp end of the question of how best to manage interpersonal data. Their response has been *Amazon Household* and *Google Families*. These are a set of interlinked user accounts with prescribed relationships - specific adult, teen and child arrangements - through which the smart home and its data are to be managed. In doing so, they create what we refer to as 'platform families'[16] - domestic kinship groups which are constituted within proprietary digital systems.

At root, these interlinked accounts comprise of taxonomies defining relationships between different users, devices, and services. Amazon separates Household into three roles: Adults (18-), Teens (13-17), Children (-12). *Google Families* also consist of three roles, but these are Parents, Family Members, and Family Manager. *Household* allows for ten members - two Adults, four Teens, four Children; *Families* allows for six. Children/Family Member accounts allow for only limited agency,

[12] 'Incognito' or 'private' browsing windows do not store browsing history and related cookies locally, preventing subsequent users from tracking activities.

[13] Alice Marwick, 'The Public Domain: Surveillance in Everyday Life', *Surveillance & Society* (2012) 9. 10.24908/ss.v9i4.4342.

[14] A.E. Marwick and Danah Boyd, 'Networked privacy: How teenagers negotiate context in social media', *New Media & Society* (2014) *16*(7), 1051–1067. https://doi.org/10.1177/1461444814543995.

[15] Peter Tolmie & Andy Crabtree, 'The practical politics of sharing personal data', *Personal Ubiquitous Computing* (2018) 22: 293. https://doi.org/10.1007/s00779-017-1071-8.

[16] (Goulden *forthcoming*)

and Adults/Parents can set limits on what media and services they can access, and when. Amazon's Teen accounts do not have these constraints, and can make purchases through Amazon using the family payment option, but orders must be reviewed by an Adult before they can be executed. Google's Family Manager role, alongside parental controls, also has executive functions including "*Decide who is in the family group*", and "*Delete the family group*". Then there are the restrictions, for example *Families'* members must all reside in the same country, and can only be a member of one family at a time. *Household* defines Adults as over 18, except in Japan where they are over 20, because this is the age at which Japanese can hold a credit card. These taxonomies, including the relationships they encode, and the limitations placed around them, are the result of a set of culturally, commercially and legally informed choices by designers - about what family looks like - and as such are inherently ethical acts.[17]

Whilst seeking to manage the challenges of interpersonal data, the deployment of tools such as *Families* and *Household* do much more. By intervening in both the information available between members, and the agency and accountability members hold over smart devices in the home, and by extension other users of those devices, they mark a radical intervention into domestic life, seeking to digitise domestic interpersonal relations. In doing so, they demonstrate how IoT technologies carry novel implications for interpersonal relations, and the data generated around them. This is the context in which data will be evaluated as 'good', or otherwise.

Legal Perspectives on Interpersonal Data & Smart Homes

Domestic IoT technologies, and the platform families they establish, intervene in a space that, historically, law has been reticent to enter. Data protection law provide rights for individuals over their own data but deal less effectively with group or collective rights.[18] Furthermore, human rights law has long recognised a right to private and family life, and any limitations on privacy need to be proportionate, necessary and legally justified, showing the value placed on keeping the home free from external privacy intrusions.[19,20,21] Similarly, EU data protection laws exempt data processing carried out by individuals during purely household or personal activities,[22] meaning they are not classified as 'data controllers' with the responsibilities that come with it. However, the growth of smart homes as ad-hoc collections of smart devices is complicating this, with case law that narrows this exemption and bringing data protection law into the home, and reframing family dynamics by potentially forcing members into managing their legal obligations internally.[23,24]

In this section, we consider a number of questions that are raised when we apply current data protection law to smart home environments. However, like with technology, law can be a blunt instrument as it needs to be contextualised. Given the focus on regulation through technology design in the GDPR, the way legal requirements are built into technology need to account for the context of

[17] Geoffrey C. Bowker & Susan Leigh Star, *'Sorting Things Out'*, MIT Press 2000.

[18] Linnet Taylor, Luciano Floridi, Bart van der Sloot, *'Group Privacy: New Challenges of Data Technologies'*, Springer 2017,

[19] Article 8, European Convention on Human Right.

[20] United Nations Declaration on Human Rights.

[21] African Charter on Human and Peoples' Rights.

[22] Article 2(2)(c), General Data Protection Regulation 2016.

[23] EU European Court of Justice - Case C212/23; Lindqvist, 2003.

[24] EU European Court of Justice - C101/01; Rynes, 2014.

use and needs of users better, particularly in the home. At one more technical level, actually embedding legal principles into technology is complex due to the importance of interpretation and law being language based, requiring translation and assumptions about meaning of terms: something that is technically difficult to account for. At another, targeting the designers and developers of IoT to support their understanding and engagement with legal requirements has its own problems around comprehension and accessibility of language.[25] However, even if these challenges could be addressed, the variety of deployment settings for these technologies mean challenges will arise that were not foreseen during the design stage. Regulation through design may have good intentions to address the lag between legal regulation and technological innovation, but it needs to attend to the way these systems are used in practice too. In homes, this could mean making a system too transparent where inferences about daily life are made trackable and visible to co-habitants, leading to social surveillance. Or perhaps setting up accounts where permissions over data processing prevent control by some household members, despite data being co-constructed and interpersonal. As the law normally does not go into this space, the appropriate responses remain to be seen, but it is important to consider in more detail some of the challenges below, in order to open up the problem space.

Who owns interpersonal data, what are their rights, and who is responsible for fulfilling them?

Even if members seek to exercise legal rights over interpersonal data, because such data does not relate to just one individual, understanding to what extent new individual data rights in Europe for GDPR apply is problematic. Rights to data portability[26] or to be forgotten[27] are already technically complex to exercise, but when data relates not just to one person, but to many, it adds another layer of difficulty. With the right to data portability, for example, it applies to raw data, but not any statistical inferences or analysis made, perhaps to provide personalisation. Thus if someone leaves the family home, they may not have a right to the personalisation of the home's devices, such as the smart thermostat's heating profile which is tailored to their activities.

A related challenge is determining who the rights may be exercised against. Smart home technologies create opacity around data flows, coupled with a complex ecosystem of stakeholders seeking access to the data. This is legally challenging, as accountability is often lacking.[28][29] There are difficulties establishing who is legally responsible, and who users need to contact to exercise their rights. As mentioned above, by bringing IoT devices into the home, there is increasing volume of domestic personal data processing ongoing, which threatens the household exemption. This may give rise to a new class of 'domestic personal data controllers' (DPDC) who might need to respond to right to be forgotten claims for smart fridge consumption by family friends or to create consent notices for babysitters captured on their Nest cams.

---

[25] Ewa Luger, Lachlan Urquhart, Tom Rodden, Mike Golembewski, 'Playing the Legal Card', *Proceedings of ACM SIGCHI 2015*. 457-466.

[26] Article 20, General Data Protection Regulation 2016.

[27] Article 17, General Data Protection Regulation 2016.

[28] Lachlan Urquhart, Tom Lodge and Andy Crabtree, *'Demonstrably Doing Accountability in the Internet of Things'*, *International Journal of Law and Technology*, (2018) Forthcoming issue

[29] Lachlan Urquhart and Tom Rodden, 'New directions in information technology law: learning from human–computer interaction', *International Review of Law, Computers & Technology*, (2017) 31:2,150-169, DOI: 10.1080/13600869.2017.1298501.

There is a tension in how they might reconcile their social obligations, as members of the household, with legalistic requirements of responding to rights requests. As gatekeepers to the home, DPDCs are also mediating data flows internally and externally. Given the current business model, data on Nest Cam or a fridge does not stay within the confines of the home, it travels to the cloud. This is particularly problematic for interpersonal data, as unlike within individual personal data that is wholly within the realm of GDPR, the law is not as clear on protection of co-constructed data or even group privacy as a whole.

This poses issues for the family unit in smart homes, especially over time. Navigating what rights individuals have and against whom becomes a complex exercise. Can children apply for subject access requests for data processing to their parents? Can family visitors demand a right to be forgotten when they leave the home? These challenges are exacerbated when family dynamics are tested by disruption (break-ups, divorce, domestic violence etc). How do DPDCs manage these issues if they are proximate to data subjects? They may find themselves having to balance legal responsibilities against the normative expectations attached to their roles within the family unit, potentially having to choose between risking censure from either the law or their loved ones.

Who can access the data?

Often with IoT, to be more legally compliant, trustworthy & responsible, the proposed solution is to increase transparency and accountability around data flows to end users.[30] The smart home is no exception, however, how accountability is managed needs to account for the domestic order. Disclosure of information within relationships may cause harm, especially during times of disruption. Information collection is fractured and distributed across smart home devices. How and if this information is presented to different family members can impact relationships and even lead to privacy harms, as in the example we began this chapter with. Given many IoT services are mediated by contracts and accounts, family members beyond the lead account holder may have limited rights. If privacy harms occur to spouses, partners or children through information sharing, they may have no recourse as they are not account holders.

Design Fictions - Domestic Data, Good and Bad

Design fiction is the practice of exploring possible futures by creating speculative and provocative fictional narratives. Here we use design fiction to create scenarios around data in the home which integrate legal, sociological and IT perspectives, and these help us both to understand what it will be like to live with future technologies, but also to think more carefully about that future.[31]

Bad Data

Fiction 1: *For that Special Someone*

Susan and Bill Anderson live with their children Josh and Angela. They have recently signed up for the FutureHome Smart Ecosystem™. This package interconnects practically all electronic devices in the home, from appliances like the TV and the oven down to electric toothbrushes. It also includes home

[30] Articles 5(2), 12, 15, General Data Protection Regulation 2016.

[31] Paul Coulton, Joseph Lindley and Rachel Cooper, *'The Little Book of Design Fiction for the Internet of Things'*, 2018, https://www.petrashub.org/the-little-book-of-design-fiction-for-the-internet-of-things/.

security devices like internal and external cameras. In order to save money on the installation, the family sign up for the AdConnect package. This package is billed as a "*data-driven brand loyalty discount package*": by sharing their data and delegating some control of the smart home to third parties, significant savings can be made on the package price.

AdConnect™ utilises interpersonal advertising, algorithmically combining user preference data with data on family relationship and events. When, on the eve of Bill's birthday, the family is targeted with ads promoting vouchers for a seedy motel on the edge of town, the kids see mum get really mad and shout at dad a lot. As the AdConnect™ package stipulates a minimum spend for all family occasions, dad still gets a present, but Angela notices he doesn't look that happy about the PieceOfMind™ location tracker that mum says he will have on him the whole time from now on.

Fiction 2: *Watching Me Watching You*

John and Mary are an estranged couple with three kids. Several months ago, John moved out of the family home where Mary and the children still live. The house was bought new three years ago with a full complement of smart devices. It still has 25 years on the mortgage. John, Mary and the children are all registered to a Kinship™ group account on the platform that controls the smart house. It was John that set up the group account originally, and his remains the admin account. As such he has executive control over the both home devices, and user privileges.

One evening in his rented flat John notices the *Ironman* film he was planning to watch has already been viewed. Mary would normally never choose to watch action films. John starts monitoring the devices in the house, noting when Mary turns the lights off at night, uses the shower, has the oven turned on long enough that John figures she must be cooking for someone else. He remembers the doorbell has a video camera feed, and starts watching it on his laptop when he gets in from work. The next Sunday when he picks up the kids from Mary he asks her why the electric toothbrush was used twice the night before. Mary tells him to leave. The next day she speaks to her lawyer, but she says as John is still paying half the mortgage he has a case for continuing to control the Kinship™ account. Instead she has an idea. On Wednesday morning, John receives a letter. Inside is a Subject Access Request - as Data Controller, he has 72 hours to catalogue all data he is holding on Susan. Failure to comply with the request in the inventory format could result in a fine of €20m or 4% of his global annual turnover, whichever is the greater. John calls his lawyer.

Fiction 3: *Equality in the Eyes of the IoT*

A legal case comes before the Supreme Court, concerning the abuse of smart home data during a family breakup. The Court creates new case law in its finding that the admin account holder is indeed a data controller, and thus under the terms of the GDPR is liable for sizeable fines. Furthermore, the co-defendant, Kinship™ LLC, is also found guilty of selling software that was judged to be non-compliant.

Even as Kinship™ lawyers prepare an appeal, the company stock price tanks, as does those of its competitors. Within days, software updates to smart homes are being issued which attempt to head off further legal action. Families across the continent wake to find that all members of the family have been granted equal status by the digital systems running the home. The continuing operation of all smart devices in the home now requires the consent of all family members. The manufacturers believe that this requirement gives their systems the utmost compatibility with legal requirements.

For the Anderson family parents, life suddenly becomes more a lot more complicated. Angela and Josh quickly realise their new found powers. Josh manages to get them off school for a whole morning, just by refusing to accept the Terms and Conditions of the front door's smart lock. Angela discovers the Restricted section of mum's video library, and learns a great deal from it. She does worry about getting caught by one of her parents coming home early, but the risk is lowered by the fact that she can now access dad's PieceOfMind tracker, and see where he is at all times. All in all, the kids are very pleased with their newfound privileges.

Good Data

Fiction 4: *Smart Home Truths*

Sam and Leslie have just moved in together. Leslie loves new tech, and has already outfitted the house with the latest IoT gadgets and smart control system. In order to fully use the integrated system each occupant needs to be registered as a user in the system although basic functionality, such as changing TV channels and switching on and off lights, is still available to an unregistered user. Leslie fails to register Sam as a user, always seeming to not get round to doing it. A year later, the system still only recognises Sam as a "guest", not a partner.

Sam can't seem to get on with the smart home. Leslie has to choose the music to play as only official family members have access to the house's media library. Other things keep happening. Sometimes the smart shower switches to cold when Sam is using it and refuses to alter temperature, or the washing machine somehow uses the wrong profile and ruins Sam's delicate clothing. Leslie tells Sam that it's all in their head, and that they are fantasizing that they're being persecuted by the smart home.

When Leslie's out at work, Sam's old friend Alex stops by for a long overdue cup of tea, and a tearful Sam confesses that they feel they're losing the plot. Alex thinks something sounds very wrong, and convinces Sam to request a SafePersonalDataAudit from the smart home company. She does so by using utility bills and government records to evidence her membership of the home. The audit exhaustively logs every action Leslie has taken on the system, revealing a campaign of control and coercion, effectively weaponizing the smart home against Sam. Sam packs a bag. The doorbell camera glares balefully as Sam and Alex depart.

Fiction 5: *Machine Learning Magic*

Susan and Bill Anderson are having marital problems. Having come to suspect Bill of having an affair, Susan has grown distant. Their sex life is almost non-existent, and Susan has turned to online pornography as a means of finding satisfaction. Bill has noticed his wife's distance but finds himself unable to initiate a conversation about it, fearful about where it might lead. Each carries on going through the motions, unable or unwilling to address the dark cloud hanging over them.

Part of the Anderson's installed FutureHome Smart Ecosystem™ is an inbuilt recommender system - Synygy™. Unlike traditional systems designed around individual users (inevitably resulting in parents being pestered with recommendations for their kids' favourite cartoons), Synygy is designed to not only recognise multiple users, but to use machine learning to identify from their individual preferences, content that would appeal to any subset of them, if and when they sit down to watch together.

Bill and Susan often spend some time after the children have gone to bed in the living room, watching television - it's a way of being together without actually having to talk. At first, some of Synygy's suggestions make Susan uncomfortable, because they clearly drawn on some of her viewing habits which she wishes to keep private. However, Synygy promotes the inclusion of 'wildcard' content into its suggestions, and is explicit to users that is it doing so - without identifying which recommendations specifically. Susan knows full well that its suggestion of *Visit from the Plumber Vol.III* isn't a wildcard, but it is easy enough to confirm Bill's belief that it is. They share a rare joke about how stupid this recommender systems are.

Drawing on their full viewing profiles, their demographics, and fine-grained data on daily routines as captured by Smart Ecosystem, and combining it with its full user base datasets, Synygy begins to suggest both romantic films and films that reflect the Anderson's current domestic turbulence. The shared experiences that follow generate some uncomfortable moments on the Anderson sofa, but over the weeks Bill and Susan begin to talk, properly, for the first time in months.

What Makes Good Domestic Data, Good?

The rise of the Internet of Things marks the latest chapter in Weiser's[32] ubiquitous computing vision of the "disappearing computer". Formerly innocuous devices such as toothbrushes, thermostats, televisions, speakers and even dolls[33] are now imbued with so-called "smart" functionality, ostensibly harnessing the power of the digital but more specifically the "good" that can be leveraged from reasoning about data at scale to enhance previously mundane household activities and to enable new experiences. Furthermore, while previously operating as a collection of disparate artefacts, the voice interfaces of Google Home and Amazon Echo seek to make sense of, unify and integrate this ecosystem of devices into an ad-hoc infrastructure for the modern smart home. The end-game of this trajectory is currently uncertain. In the above we have used design fiction to explore possible future interactions between social, legal and technical systems in this place; three we have labelled as 'bad data'; two 'good'. However, even within these short scenarios the picture is more complicated. We argue that the data itself in these fictions is agnostic, and is only meaningful when considered in a broader socio-legal-technical context. Our goal with the Fictions was not to present answers, but to open up questions.

Our data fictions are deliberately playful, but all are plausible. Fiction 1 demonstrates how the most ostensibly mundane of data implicitly has the potential to be momentous because, when it comes to data about the situated arrangements of tight-knit groups, *meaning is in the eye of the beholder*. What may appear in one domestic context unremarkable may in another be revelatory, and vice versa.[34] This Fiction also highlights how data itself does not have to be exposed to be consequential, instead here it is the output of algorithmically-processed data which is read as being revealing of moral impropriety. This scenario points at the commercial imperatives that are often at play here,

[32] Mark Weiser, 'The computer for the 21st century'. *SIGMOBILE Mobile Computing and Communications,* Rev. 3, 3 (July 1999), 3-11. DOI=http://dx.doi.org/10.1145/329124.329126.

[33] Wolf Richter, 'Our Dental Insurance Sent us "Free" Internet-Connected Toothbrushes. And this is What Happened Next', Wolf Street, 14 Aprill 2018, https://wolfstreet.com/2018/04/14/our-dental-insurance-sent-us-free-internet-connected-toothbrushes-and-this-is-what-happened-next/.

[34] Goulden, Murray, Peter Tolmie, Richard Mortier, Tom Lodge, Anna-Kaisa Pietilainen, and Renata Teixeira. 2018. "Living with Interpersonal Data: Observability and Accountability in the Age of Pervasive ICT." *New Media & Society* 20 (4): 1580–99.

which can drive the generation of potentially revealing interpersonal data. Interest in such possibilities has already been shown - Facebook announced, in 2017, that it was going to begin to enable the targeting of advertising at family groups[35]. There are potentially considerable conflicts between the commercial interests of industry, and those of smart home occupants, and a real danger that careless, or simply short-termist approaches to developing the smart home ultimately result in the kind of toxicity which has now surrounded Facebook, in the form of fake news and the Cambridge Analytica scandal, during 2017-18. We must hope that the technology industry learns from its current travails, if only for its own long-term self-interest.

Fiction 2 focuses on how kinship groups' membership and roles are dynamic, both changing gradually with the unfolding of time, but also occasionally in great lurches. This has profound implications for the intimate data which accumulates around such relationships, and how control over it is maintained.[36] Similarly to Fiction 1, it shows how data from the most quotidian of objects - like toothbrushes and ovens - can be imbued with critical meaning by users interpreting data through the prism of past experience and current belief. The current design of platform families does not suggest due care is being exercised here - Amazon Household, for example, allows either Parent to remove their partner account from the family, but the agency to do so is reserved solely for those who click first - once out, the ejected is powerless to return.

At the heart of Fiction 3 is the current uncertainty regarding how regulatory frameworks, with their household exemptions, will apply to a technology platform that renders the boundaries between home and world outside so porous as to be almost meaningless. The absurd outcome of the court case points to a very good reason why the law may be reciticent to intervene in the home, namely its bluntness as an instrument in comparison to the nuances of situated domestic practices, a challenge that faces technology designers too, albeit arguably to a lesser degree. The scenario also flags the capacity of these systems, through remote updates, to change form and function literally overnight, and how consequential such changes might be[37] when the technologies involved are fully embedded in domestic life.

Fiction 4 has similarities to 2, describing an abusive partner denying their victim control over many aspects of their shared physical-digital lives, purely by exploiting administrative privileges[38]. One way in which it differs is in how accountability is established between members. In Fiction 2 Mary *can* ultimately use the law to turn the tables on John's intrusions, but only in a way in which it was not intended. In Fiction 4 by contrast Sam is able to access the devices' logs via a mechanism designed for such purposes, by presenting evidence of her occupancy of the home. Users are both empowered and marginalised by data, to both positive and negative affect.

Fiction 5 demonstrates how situated such evaluations of good or bad must be. In contrast to 1, where Bill is made accountable by data for his infidelity, the systems here allow those implicated by

---

[35] Marty Swant, Facebook Will Soon Let Brands Target Ads at Entire Families or Specific People Within Households, Adweek, 27 June 2017, https://www.adweek.com/digital/facebook-will-soon-let-brands-target-ads-at-entire-families-or-specific-people-within-households/..

[36] Jimmie Manning and Danielle M. Stern. 'Heteronormative Bodies, Queer Futures: Toward a Theory of Interpersonal Panopticism.' *Information, Communication & Society 21*, no. 2 (February 1, 2018): 208–23. https://doi.org/10.1080/1369118X.2016.1271901.

[37] The inspiration for this element of the scenario comes from the news in 2017 that a remotely-issued firmware update bricked several hundred Lockstate customers' door locks. Iain Thomson, 'Firmware update blunder bricks hundreds of home 'smart' locks', *The Register*, 11 September 2017, 'https://www.theregister.co.uk/2017/08/11/lockstate_bricks_smart_locks_with_dumb_firmware_upgrade/.

[38] (Goulden *forthcoming*)

the exposure of personal data a means of deflecting their accountability. Unlike the advertising system which incriminates Bill, Synygy explicitly includes wildcard suggestions, which in this instance act as 'noise' which Susan can appropriate to hide what she wants to keep hidden. Accountability is itself nuanced - whilst we label as good Susan's avoidance of it, we apply the same label to Leslie's exposure in Fiction 4. This particular distinction hinges on the actions in question, one set - Susan's - which we judged to be personal, the other - Leslie's - we judged to require disclosure. Our justification relies on the impact of Leslie's actions on Sam, but nevertheless these are normative judgements that we make, and must be reflexive of, just as designers should be.

These Fictions raise difficult moral questions, which the terminology of 'good' data invokes. The reader might see it as justifiable that Susan's pornography tastes are hidden, but have little sympathy when similar systems reveal Bill's infidelity. In an intimate space such as the home, inevitably smart technologies impinge on normative judgments of behaviour. As Bowker & Star[39] remind us, the decisions of the designs of these systems are always ethical in nature. There is no single standardised solution for designing smart domestic technologies, but an awareness of what is at stake, and when individual's right to privacy may conflict with another's right to know, is necessary. In portraying Synygy's recommendations altering Susan and Bill's relationship, Fiction 5 also poses a question of political philosophy. How should we think about such systems using use algorithmic processing to change our behaviour? Synygy is not directed by a human designer to rescue their marriage, but here the algorithms' goal of getting them to watch content has that effect. Does the fact that the outcome could be considered positive make this unambiguously good data? Is the fact that it is unintentional rather than by design important - would the alternative be creepily paternalistic? Does our response change if the algorithm has negative impacts on users - as many systems have been shown to?[40]

Conclusion

With little regulatory oversight, the technology industry has propelled societies towards a ubiquitous, 'smart' future, one that was barely conceivable at the turn of the millennium. However, the wholesale application of these technologies in disciplinary isolation may lead to unforeseen social impacts, both good and bad, or more likely impossibly difficult to characterise so simply, but potentially risking very real harms. The IoT-enabled home industry is built upon but also hopelessly addicted to data, and the distributed nature of ambient data collection means there that we are quickly becoming surrounded by digital ears. There are many concerns to be raised about how the companies which own those ears are monetising what they hear, whether that be Amazon selling transcripts of our conversations with Alexa[41] or Roomba selling the floor plans of our homes[42]. Here though our focus has been on the dangers of interpersonal data. We would argue that data is agnostic, that it is neither good nor bad – but rather that the Internet of Things enables vastly powerful tools that can reason about data created by "the user" but also complicated by, as we have seen, data about others. Activities in the home are inextricably linked with the activities of other

[39] Geoffrey C. Bowker & Susan Leigh Star, 'Sorting Things Out', MIT Press 2000.

[40] Eubanks, Virginia. 2018. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. New York, NY: Macmillan USA.

[41] Rob LeFebvre, 'Amazon may give developers your private Alexa transcripts', Engadget Blog, 7 July 2017, https://www.engadget.com/2017/07/12/amazon-developers-private-alexa-transcripts/.

[42] Natalie O'Neill, 'Roomba maker wants to sell your home's floor plan', NYPost, 25 July 2017, https://nypost.com/2017/07/25/roomba-maker-wants-to-sell-your-homes-floor-plan/.

family members, and this is a point we believe is largely overlooked by the current crop of smart devices. Whether considering the commercial interests of the technology company seeking a foothold into the domestic space through data analysis at scale, or the privacy of the teenage daughter's purchases via the shared Amazon account, these data driven technologies must respect interpersonal relationships, and the distribution of agency amongst them, both socially and legally. They must also, in doing so, recognise the moral choices they are making in involving themselves in these spaces, and redefining their possibilities.

Information privacy law traditionally stops at the front-door of the home. It is not clear whether data protection law provides redress for the actual harms faced by the occupants of the modern smart home, or whether it is too far removed from the practical challenges faced by users – however in the interim compliance mechanisms like privacy by design[43] are bringing it in by the backdoor. If technology embeds regulatory norms,[44] these can structure relationships in the home. Even if done with the best of intentions, these are external interventions into complex, intimate spaces, and the consequences of them are difficult to anticipate. The extent to which they are negotiable or legible to end users, and compliant with the situated norms of any particular household, will affect their impact. A good example is requirements for parents to consent on behalf of under-16s to access services like social media or online shopping.[45] Depending on family dynamics, such a requirement may impact autonomy and agency of young people in negative ways, and neglect developmental differences of different users.

Our conclusion, then, is to suggest that for the Internet of Things and the smart home to be considered as "good" – or rather, harmless – in their use of data, they must be grounded in an interdisciplinary conversation about the tensions at the intersection of human-computer interaction, or increasingly human-data interaction[46], the social life of the home and the law. There are significant implications for the designers of technologies of the future smart home:

- The next generation of smart devices should, potentially actively and disruptively, deliver data protection norms into the home, perhaps by considering what a meaningful and recognisable digital front-door should look like.
- They must involve their users in a legitimate conversation about the value of their data – not just engaging in privacy by design, but affording *informed and visible* transactions around data that can be integrated into the socially negotiated work of the home.
- Where interpersonal data is concerned, its visibility, and the potential accountabilities that flow from that for those implicated by it, requires careful thought on the part of designers. Predicting all outcomes is impossible, but certain data, in certain systems, may require the maintenance of *personal* privacy, even where that undermines the possibilities presented by merging user data. In other situations, the deliberate, and explicit, insertion of noise into the data may offer a solution which mediates between individual and group interests.
- Technology blunders into ordering the home in different ways. We need to better understand the implications of using technology design to bring structural and legal norms into the 'sacred space' of the home. The smart home should be made configurable, not seek

[43] Article 25, General Data Protection Regulation 2016.

[44] Lawrence Lessig, *'Code v2'*, http://codev2.cc/download+remix/Lessig-Codev2.pdf.

[45] Article 8, General Data Protection Regulation 2016.

[46] Richard Mortier, Hamed Haddadi, Tristan Henderson, Derek McAuley and Jon Crowcroft, 'Human-Data Interaction: The Human Face of the Data-Driven Society' (October 1, 2014), https://ssrn.com/abstract=2508051 or http://dx.doi.org/10.2139/ssrn.2508051.

to configure, the family schema to reflect the complex, fluid and inherently non-standard domestic environment.

Finally, we consider how some of the challenges we have raised can and are beginning to be addressed through research and design.

Human-Computer Interaction (HCI), and its focus on user centric design, can address some of these regulatory challenges by surfacing social practices and how users orientate around a technology. Furthermore, the growing interest in embedding socially desirable values and norms into technology is one approach to addressing the risks of bad data. However, in practice, as phenomenologists such as Don Ihde have argued for a long time, how a technology is designed and how it is used differ considerably.[47]

Technologies designed for one purpose can be be repurposed for another. So whilst a smart camera entry system can be designed to spot intruders, it can also be used to track movements of a spouse, to question on why they are arriving so late. A smart thermostat can be used to help users manage energy more efficiently, but it can also be used by social workers to argue a house was too cold, showing evidence of neglect of children. A smart fridge can be used to manage consumption of food to address waste, but it can also be a trigger for those with eating disorders by questioning their consumption practices.

Many of these technologies assume social harmony within the home, in the same way socio-technical research in the early years of Computer-Supported Cooperative Work (CSCW) research often assumed harmony between worker and employer when new systems were deployed. As more critical school lines of thought emerged, particularly in Scandinavia, this assumption was challenged and a more conflict driven model of the setting for technology deployment was given attention. For the smart home, the complexity needs attention. The power relationships and domestic hierarchies cannot be neglected in design.

Relatedly, there is a risk in this design space of the assumption that social problems can be fixed by technology. Without considering the context of deployment, ostensibly good data applications can fall into bad data. Accordingly, the fallacy of a binary good/bad is not productive when designing for the home, and arguably for any data driven technology that humans interact with. It neglects the subtleties, and how people use and domesticate technologies into their everyday lives.

Furthermore, with its focus on individual rights, for example in data protection, the law can also neglect these subtleties. Data in homes is often co-constructed, yet protection is constrained to individualised notions of one user, one device. This is not the case, and whilst the home is posing challenges for technology design, equally the law will need to face up to the limitations of not attending to the social context of use too. Privacy by design is a good idea in the abstract, but if the protections, or understanding of what is needed do not tally with the reality, then these safeguards are likely to miss the mark.

If designers cannot give these questions the attention they require, or resolve them in a way that does not place all implicated members interests over primarily commercial interests, the ethical choice is to not pursue the smart home at all.

References

- African Charter on Human and Peoples' Rights.

[47] Don Ihde, '*Technology and the Lifeworld: From Garden to Earth*', Indiana University Press, 1990

- Article 8, European Convention on Human Right.
- Articles 2(2)(c), 5(2), 8,12, 15, 17, 20, and 25, General Data Protection Regulation 2016.
- Geoffrey C. Bowker & Susan Leigh Star, 'Sorting Things Out', MIT Press 2000.
- Deborah Chambers, 'A Sociology of Family Life', Polity Press 2012.
- David Cheal, 'Sociology of Family Life', Springer 2002.
- Paul Coulton, Joseph Lindley and Rachel Cooper, 'The Little Book of Design Fiction for the Internet of Things', 2018, https://www.petrashub.org/the-little-book-of-design-fiction-for-the-internet-of-things/.
- EU European Court of Justice - Case C212/23; Lindqvist, 2003.
- EU European Court of Justice - C101/01; Rynes, 2014
- (Goulden forthcoming)
- Goulden, Murray, Peter Tolmie, Richard Mortier, Tom Lodge, Anna-Kaisa Pietilainen, and Renata Teixeira. 2018. "Living with Interpersonal Data: Observability and Accountability in the Age of Pervasive ICT." New Media & Society 20 (4): 1580–99.
- Don Ihde, 'Technology and the Lifeworld: From Garden to Earth', Indiana University Press, 1990
- Bret Kinsella, 'Smart Speakers to Reach 100 Million Installed Base Worldwide in 2018, Google to Catch Amazon by 2022', *Voicebot AI Blog*, 10 July 2018, https://voicebot.ai/2018/07/10/smart-speakers-to-reach-100-million-installed-base-worldwide-in-2018-google-to-catch-amazon-by-2022/
- Tom Lammont, 'Life after the Ashley Madison affair', *The Observer*, 28 February 2016, https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked.
- Rob LeFebvre, 'Amazon may give developers your private Alexa transcripts', *Engadget Blog*, 7 July 2017, https://www.engadget.com/2017/07/12/amazon-developers-private-alexa-transcripts/.
- Ewa Luger, Lachlan Urquhart, Tom Rodden, Mike Golembewski, 'Playing the Legal Card', Proceedings of ACM SIGCHI 2015. 457-466.
- Lawrence Lessig, 'Code v2', http://codev2.cc/download+remix/Lessig-Codev2.pdf.
- Jimmie Manning and Danielle M. Stern. 'Heteronormative Bodies, Queer Futures: Toward a Theory of Interpersonal Panopticism.' Information, Communication & Society 21, no. 2 (February 1, 2018): 208–23. https://doi.org/10.1080/1369118X.2016.1271901.
- Alice Marwick, 'The Public Domain: Surveillance in Everyday Life', Surveillance & Society (2012) 9. 10.24908/ss.v9i4.4342.
- A.E. Marwick and Danah Boyd, 'Networked privacy: How teenagers negotiate context in social media', New Media & Society (2014) 16(7), 1051–1067. https://doi.org/10.1177/1461444814543995.
- David Morgan, 'Family Connections: An Introduction to Family Studies', Polity Press 1996.
- Richard Mortier, Hamed Haddadi, Tristan Henderson, Derek McAuley and Jon Crowcroft, 'Human-Data Interaction: The Human Face of the Data-Driven Society' (October 1, 2014), https://ssrn.com/abstract=2508051 or http://dx.doi.org/10.2139/ssrn.2508051.
- Helen Nissenbaum, 'Privacy As Contextual Integrity', Washington Law Review (2004): 79.
- Natalie O'Neill, 'Roomba maker wants to sell your home's floor plan', *NYPost*, 25 July 2017, https://nypost.com/2017/07/25/roomba-maker-wants-to-sell-your-homes-floor-plan/.
- Jamie Orme, 'Samaritans pulls 'suicide watch' Radar app over privacy concerns', *The Guardian*, 7 November 2014, https://www.theguardian.com/society/2014/nov/07/samaritans-radar-app-suicide-watch-privacy-twitter-users.

- Talcot Parsons, ‘The American Family’, in Talcot Parsons and Robert Freed Bales, Family, socialization and interaction process. Free Press, 1955.
- Associated Press, ‘Smart Speaker Sales More Than Triple in 2017’, *Billboard*, 28 December 2017, https://www.billboard.com/articles/business/8085524/smart-speaker-sales-tripled-25-million-year-2017.
- Wolf Richter, ’Our Dental Insurance Sent us “Free” Internet-Connected Toothbrushes. And this is What Happened Next’, *Wolf Street*, 14 Aprill 2018, https://wolfstreet.com/2018/04/14/our-dental-insurance-sent-us-free-internet-connected-toothbrushes-and-this-is-what-happened-next/.
- Linnet Taylor, Luciano Floridi, Bart van der Sloot, ‘Group Privacy: New Challenges of Data Technologies’, Springer 2017,
- Marty Swant, Facebook Will Soon Let Brands Target Ads at Entire Families or Specific People Within Households, *Adweek*, 27 June 2017, https://www.adweek.com/digital/facebook-will-soon-let-brands-target-ads-at-entire-families-or-specific-people-within-households/.
- Iain Thomson, ‘Firmware update blunder bricks hundreds of home 'smart' locks’, *The Register*, 11 September 2017, ‘https://www.theregister.co.uk/2017/08/11/lockstate_bricks_smart_locks_with_dumb_firmware_upgrade/.
- Peter Tolmie & Andy Crabtree, ‘The practical politics of sharing personal data‘, Personal Ubiquitous Computing (2018) 22: 293. https://doi.org/10.1007/s00779-017-1071-8.
- United Nations Declaration on Human Rights.
- Lachlan Urquhart, Tom Lodge and Andy Crabtree, ‘Demonstrably Doing Accountability in the Internet of Things’, International Journal of Law and Technology, (2018) Forthcoming issue
- Lachlan Urquhart and Tom Rodden, ‘New directions in information technology law: learning from human–computer interaction’, International Review of Law, Computers & Technology, (2017) 31:2,150-169, DOI: 10.1080/13600869.2017.1298501.
- Julia Wardhaugh, ‘The Unaccommodated Woman: Home, Homelessness and Identity’, The Sociological Review (2001) 47. 91 - 109. 10.1111/1467-954X.00164.
- Mark Weiser, ‘The computer for the 21st century’. SIGMOBILE Mobile Computing and Communications, Rev. 3, 3 (July 1999), 3-11. DOI=http://dx.doi.org/10.1145/329124.329126.